Available online at http://www.ijasrd.org/in

International Journal of Advanced Scientific Research & Development

Vol. 02, Iss. 02, Ver. I, Apr – Jun' 2015, pp. 08 – 14

e-ISSN: 2395-6089
p-ISSN: 2394-8906

A NOVEL FRAMEWORK FOR SECURE SHARING OF PERSONAL HEALTH RECORDS (PHR) IN CLOUD COMPUTING

B. Sangeetha[1]
E. Saranya[1]
G. Saranya[1]

[1] Assistant Professor, Department of CSE, Sir Issac Newton College of Engineering and Technology, Nagapattinam, India

ARTICLE INFO

Article History:

Received: 17 May 2015;
Received in revised form: 20 May 2015;
Accepted: 20 May 2015;
Published online: 30 Jun 2015.

Key words:

Personal Health Records (PHR), Cloud Computing, Data Privacy, Fine-Grained Access Control, Attribute-Based Encryption (ABE)

ABSTRACT

Online personal health record (PHR) enables patients to manage their own medical records in a centralized way, which greatly helps the storage, access and sharing of personal health data. PHR system could allow patients to better manage their health information and share it to enhance the quality and efficiency of their healthcare. Unfortunately, abuse of information stored in PHR systems will create new risks for patients, and we need to empower them to protect their health information to avoid problems such as medical identity theft. This project introduces the notion of Accountable use and updates of personal health records and design a patient-centric monitoring system based on it. Each patient encrypts his PHR data before uploading to the cloud server. However, issues such as risks of privacy exposure, flexible policy access, scalability in key management and efficient on-demand user revocation, have remained the most vital challenges to achieve secure, scalable and fine-grained data access control. To enable fine-grained and scalable access control for PHRs, we leverage attribute based encryption (ABE) techniques to encrypt each patients' PHR data. ABE applied on multi authority owner scenario that greatly reduces the key management complexity for owners and users. This proposed scheme enhances the Accountability of Personal Health Record usage via patient-centric monitoring. This scheme also enables dynamic modification of access policies or file attributes, supports efficient on-demand revocation and break-glass access under emergency scenarios.

How to cite this article: Sangeetha, B., Saranya, E., & Saranya, G., (2015). "A Novel Framework for Secure Sharing of Personal Health Records (PHR) in Cloud Computing". *International Journal of Advanced Scientific Research & Development (IJASRD), 02* (02/I), pp. 08 – 14.

INTRODUCTION

Cloud computing is a computing paradigm, where a large pool of systems are connected in private or public networks, to provide dynamically scalable infrastructure for application, data and file storage. With the advent of this technology, the cost of computation, application hosting, content storage and delivery is reduced significantly. Cloud computing is a practical approach to experience direct cost benefits and it has the potential to transform a data center from a capital-intensive set up to a variable priced environment.

In recent years, Personal Health Record (PHR) has emerged as a patient-centric model of health information exchange. PHR service allows a patient to create, delete, manage, and control her personal health data in one place through the web. Especially, each patient is promised the full control of her medical records and can share her health information with a wide range of users. Due to the high cost of building and maintaining specialized data centers, many PHR services are outsourced to third-party service providers, for example, Microsoft Health Vault[13]. Microsoft HealthVault is a web-based platform from Microsoft to store and maintain health and fitness information.

A feasible and promising approach would be to encrypt the data before outsourcing. The PHR owner herself should decide how to encrypt her files and to allow which set of users to obtain access to each file. A PHR file should only be available to the users who are given the corresponding decryption key, though remain confidential to the rest of users. Additionally, the patient shall always retain the right to not only grant, but also revoke access privileges when they feel it is necessary[2].

1.1 Literature Survey

This paper is mostly related to works in cryptographically enforced access control for outsourced data and attribute based encryption. To comprehend fine-grained access control, the traditional Public Key Encryption (PKE) based schemes[2][10] either incur high key management overhead, or require encrypting multiple copies of a file using different users' keys. To improve the scalability of the above solutions, one-to-many encryption methods such as ABE can be used.

In Goyal et. al's seminal paper on ABE[6], data is encrypted under a set of attributes so that multiple users who hold proper keys can decrypt. This potentially makes encryption and key management more efficient. An ultimate property of ABE is preventing against user collusion. In addition, the encryption is not required to know the ACL.

Recently, Narayan et al. proposed an attribute-based infrastructure for EHR systems, where each patient's health record files are encrypted using Ciphertext Policy-ABE[10] that allows direct revocation. Though, the ciphertext length grows linearly with the number of unrevoked users. In[6], a variant of ABE that allows delegation of access rights is proposed for encrypted EHRs.

Ibraimi *et.al.*[7] Applied ciphertext policy ABE (CP-ABE)[3] to manage the sharing of personal health records, and introduced the concept of social/professional domains. In[1], Akinyele et al. investigated using ABE to generate self-protecting EMRs, which can be stored on cloud servers or cellphones so that EMR could be accessed when the health provider is offline.

Yu *et al*. applied key-policy ABE to secure outsourced data in the cloud, where a single data owner can encrypt her data and share with multiple authorized users, by issuing keys to them that contain attribute-based access rights. They also propose a method for the data owner to revoke a user efficiently by delegating the updates of affected ciphertext and user secret keys to the cloud server. The key update operations can be combined over time and their scheme achieves low amortized overhead.

Chase and Chow[5] proposed a multiple-authority ABE (CC MA-ABE) solution in which multiple trusted authorities, each governing a different subset of the user attributes, generate user secret keys collectively. A user needs to acquire one part of her key from each TA. This scheme prevents against collusion among at most $N - 2$ TAs, in addition to user collusion resistance. Yet, it is not clear how to realize efficient user revocation. Since CC MA-ABE embeds the access policy with users' keys rather than the ciphertext, a direct application of it to a PHR system is non-intuitive, as it is not clear how to allow data owners to specify their file access policies.

1.1 Overview

Personal Health Record (PHR) is an emerging patient-centric model of health information exchange. A PHR services allow a patient to create, manage, delete and control her personal health information in one place through the web, which has made the storage, retrieval, access and sharing of the medical information more efficient. Due to the high cost of building and maintaining specialized data centers, many PHR services are outsourced to third-party service providers. Storing PHRs in the cloud, the patients lose physical control to their personal health data. So each patient encrypts her own PHR data before uploading to the cloud server.

The main goal of this project is achieving security, scalability, accountability and fine-grained data access Control in Cloud Computing. Online personal health record (PHR) enables patients to deal with their own medical records in a centralized way, which greatly helps the storage, access and sharing of personal health data. It could allow patients to better manage their health information and share it to enhance the quality and efficiency of their healthcare. Unfortunately, abuse of information stored in PHR systems will create new risks for patients, and we need to empower them to protect their health information to avoid problems such as medical identity theft. In this project, we introduce the notion of Accountable use and update of personal health records and design a patient-centric monitoring system based on it.

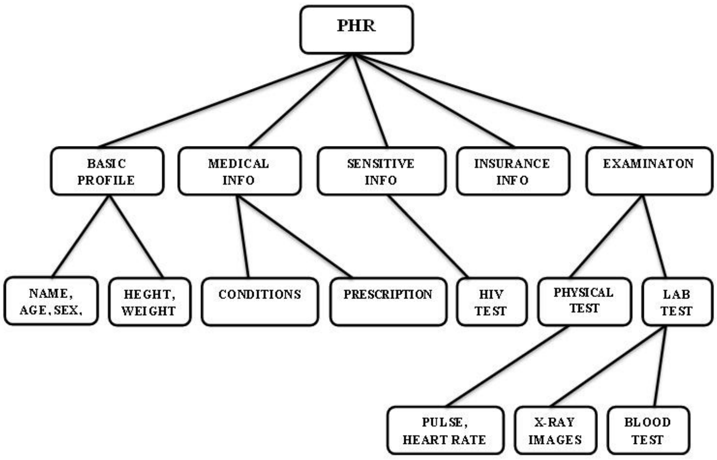

Fig.1: Attribute hierarchy of PHR

The PHR system is divided into multiple security domains namely, public domains (PUDs) and personal domains (PSDs) according to the different users‟ requirements. The personal domains (PUDs) consist of users who make access based on their professional roles, such as doctors, nurses, pharmacists and medical researchers. In a PUD multi-authority ABE is used, in which there multiple Attribute Authorities (AAs), each are governing a disjoint subset of attributes. PUD defines the Role Attributes that representing the professional role of a PUD user. Users in PUDs get their attribute-based secret keys from the attribute authorities, without directly interacting with the owners. To control access from personal domain users, owners are free to specify role-based access policies for her PHR files, though do not need to know the list of authorized users when doing encryption. Since the personal domains contain the majority of users, that greatly reduces the key management overhead for both the owners and users.

PSD users are directly associated with a data owner such as family members or close friends. Owners directly assign access privileges for personal user and encrypt a PHR file under its data attributes. In personal domain each data owner is act as a trusted authority. Data attributes are defined for PSDs, representing the intrinsic properties of the PHR data. In PSD each PHR file is labeled with its data attribute, while the key size is only linear with the number of file categories a user can access. Since the number of users in a PSD is small, it reduces the burden for the owner.

In this framework, there are multiple Security Domains (SDs), multiple owners, multiple users and multiple AAs. In addition, two ABE systems are involved: for each PSD, revocable KP-ABE scheme is used; for each PUD, revocable MA-ABE scheme is used.

SYSTEM ARCHITECTURAL DESIGN

The owners upload ABE-encrypted PHR files to the server. Each owner's PHR file is encrypted both under a certain fine grained and role-based access policy for users from the PUD to access, and under a set of data attributes that allows access from users in the PSD. Only authorized users can decrypt the PHR files, excluding the server. The data readers download PHR files from the server, and they can decrypt the files only if they have proper attribute based keys. The data contributors will be granted write access to someone's PHR, if they hold proper write keys.

2.1 System Setup and Key Distribution

The system first defines a common universe of data attributes shared by every PSD, such as "basic profile", "medical info", "prescriptions" and "conditions". An emergency attribute is also defined for break-glass access. Each PHR owner generates two keys such as public and master keys. The public keys can be published via Healthcare Social Network (HSN). There are two ways for distributing secret keys. First, PHR owner can specify the access privilege of a data reader in her PSD, and her application automatically generates and distribute corresponding key to the user. Second, a reader in PSD could get the secret key by sending a request to the PHR owner via HSN, and the owner will grant her a set of data attributes. In addition, the data attributes can be organized in a hierarchical manner for efficient policy generation. For the PUDs, the system defines role attributes, and a reader in a PUD gets secret key from AAs, which binds the user to her requested attributes/roles. MA-ABE is used to encrypt the PHRs. AAs distribute write keys that permit contributors in their PUD to write to someone PHR.

2.2 PHR Encryption and Access

The owners upload ABE-encrypted PHR files to the third party server. Each owner’s health record is encrypted both under a certain fine grained and role-based access policy for users from the PUD to access, and under a set of data attributes that allows access from users in the personal domain. Only authorized users can decrypt the PHR files, excluding the server. The data readers download PHR files from the cloud server, and they can decrypt the record only if they have proper attribute based secret keys. The data contributors will be granted write access to someone’s PHR, if they hold proper write keys.

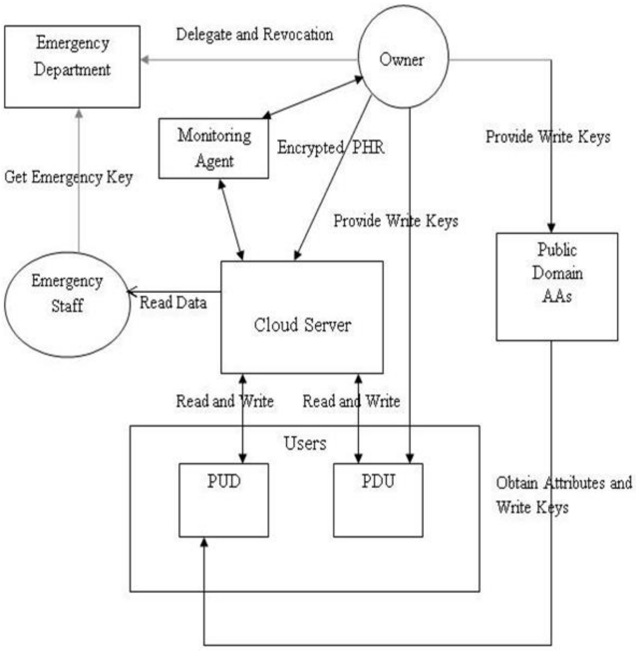

Fig.2: PHR Architecture Diagram

2.3 User Revocation

Here we consider revocation of a data reader or her attributes/access privileges. There are several possible cases: 1) Revocation of one or more role attributes of a PDU user; 2) Revocation of a public domain user; 3) Revocation of a personal domain user’s access privileges; 4) Revocation of a PDU user. These can be initiated through the PHR owner’s client application.

2.4 Policy Updates

A PHR owner can update her access policy for an existing PHR document by updating the attributes in the ciphertext. Our scheme should supports the operations include add, modify, delete, which can be done by the server.

2.5 Break-Glass

When an emergency happens, the regular access policies may no longer be valid. To handle this situation, break-glass access is needed to access the target’s PHR. In our framework, each owner’s PHR’s access right is also delegated to an emergency department (ED). To prevent from abuse of break-glass option, the emergency staff contact with ED to verify her identity and the emergency situation, and get temporary read keys. After the emergency is over, the patient can revoke the access privilege via the emergency department.

2.6 Accountable Health Record Usage

Accountable usage which allows patients to be aware of all occurrences of “meaningful usage” of their health records and Accountable update, which allows patients to be aware of updates to their health records stored on a repository, including submission of new health records by third parties such as medical professionals, as well as patients themselves. PHR owner maintain the monitoring agent to monitor the health record. Our proposed patient-centric monitoring system allows health record update and health record usage to enhance accountability in health record sharing.

CONCLUSION AND FUTURE WORK

In this work, a framework discussed for secure sharing of personal health records in cloud computing. This work introduces the notion of Accountable use and updates of personal health records and design a patient-centric monitoring system based on it. Owner encrypts her PHR and stored in third party server such as cloud provider. The proposed framework addresses the unique challenges brought by multiple PHR owners and PHR users, ABE greatly reduce the complexity of key management while enhance the privacy guarantees compared with previous works. To enable fine-grained and scalable access control for PHRs, it leverage attribute based encryption (ABE) techniques to encrypt each patient's PHR data. ABE applied on multi authority owner scenario that greatly reduces the key management complexity for owners and users. This scheme enhances the Accountability of Personal Health Record usage via patient-centric monitoring. It also enables dynamic modification of access policies or file attributes, supports efficient on-demand user revocation and break-glass access under emergency scenarios.

The future work is to enhance the MA-ABE scheme to support more expressive owner-defined access policies and efficient on-demand user revocation. The future work includes the enhancement of functionality of a patient controlled monitoring agent.

REFERENCES

[1] J. A. Akinyele, C. U. Lehmann, M. D. Green, M. W. Pagano, Z. N. J. Peterson, and A. D. Rubin (2010), "Self-protecting electronic medical records using attribute-based encryption," Cryptology ePrint Archive, Report 2010/565, 2010, http://eprint.iacr.org/.

[2] J. Benaloh, M. Chase, E. Horvitz, and K. Lauter (2009), "Patient controlled encryption: ensuring privacy of electronic medical records," in *CCSW '09*, 2009, pp. 103–114.

[3] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in *IEEE S& P '07*, 2007, pp. 321–334.

[4] A. Boldyreva, V. Goyal, and V. Kumar, "Identity-based encryption with efficient revocation," in *ACM CCS*, ser. CCS '08, 2008, pp. 417–426.

[5] M. Chase and S. S. Chow, "Improving privacy and security in multi-authority attribute-based encryption," in *CCS '09*, 2009, pp. 121130.

[6] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in *CCS'06*, 2006, pp. 89–98.

[7] L. Ibraimi, M. Petkovic, S. Nikova, P. Hartel, and W. Jonker, "Ciphertext-policy attribute-based threshold decryption with flexible delegation and revocation of user attributes," 2009.

[8] S. Jahid, P. Mittal, and N. Borisov, "Easier: Encryption-based access control in social networks with efficient revocation," in *ASIACCS*, Hong Kong, March 2011.

[9] A. Lewko and B. Waters, "Decentralizing attribute based encryption," *Advances in Cryptology–EUROCRYPT*, pp. 568–588, 2011.

[10] M. Li, S. Yu, K. Ren, and W. Lou, "Securing personal health records in cloud computing: Patient-centric and fine-grained data access control in multi-owner settings," in *SecureComm'10*, Sept. 2010, pp. 89–106.

[11] M. Li, S. Yu, N. Cao, and W. Lou, "Authorized private keyword search over encrypted personal health records in cloud computing," in *ICDCS '11*, Jun. 2011.

[12] X. Liang, R. Lu, X. Lin, and X. S. Shen, "Ciphertext policy attribute based encryption with efficient revocation," *Technical Report, University of Waterloo*, 2010.

[13] H. Lohr, A.-R. Sadeghi, and M. Winandy, "Securing the e-health cloud," in *Proceedings of the 1st ACM International Health Informatics Symposium*, ser. IHI '10, 2010, pp. 220–229.

[14] K. D. Mandl, P. Szolovits, and I. S. Kohane, "Public standards and patients' control: how to keep electronic medical records accessible but private," *BMJ*, vol. 322, no. 7281, p. 283, Feb. 2001.

[15] S. Muller, S. Katzenbeisser, and C. Eckert, "Distributed attribute based encryption," *Information Security and Cryptology–ICISC 2008*, pp. 20–36, 2009.

[16] M. Pirretti, P. Traynor, P. McDaniel, and B. Waters, "Secure attribute-based systems," *Journal of Computer Security*, vol. 18, no. 5, pp. 799–837, 2010.

[17] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable, and fine-grained data access control in cloud computing," in *IEEE INFOCOM'10*, 2010.

[18] S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute based data sharing with attribute revocation," in *ASIACCS'10*, 2010.

[19] Y. Zheng, "Key-policy attribute-based encryption scheme implementation," http://www.cnsr.ictas.vt.edu/resources.html.